IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product operable to control an e-mail client computer to detect e-mail propagated malware, said computer program product comprising:

e-mail generating logic operable to generate an e-mail message;

comparison logic operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer; and

identifying logic operable to identify whether~~said e-mail message as potentially containing malware if at least one of~~:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said identifying logic is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

quarantine queue logic operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

2. (Original) A computer program product as claimed in claim 1, wherein said e-mail message specifies a plurality of addressees, said comparison logic being operable to compare said plurality of addressees with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

3. (Original) A computer program product as claimed in claim 1, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

4. (Original) A computer program product as claimed in claim 3, wherein said proportion of addressees within said address book is user specified.

5. (Cancelled)

6. (Previously Presented) A computer program product as claimed in claim 1, wherein said quarantine period is user specified.

7. (Original) A computer program product as claimed in claim 1, comprising confirmation input logic operable when said e-mail message is identified as potentially containing malware to generate a user message seeking a confirmation input from a user of said client computer before said e-mail message is sent.

8. (Original) A computer program product as claimed in claim 1, comprising administrator warning logic operable when said e-mail message is identified as potentially containing malware to send an administrator warning message to an administrator of said client computer regarding said e-mail message.

9. (Currently Amended) A method of detecting e-mail propagated malware within an e-mail client computer, said method comprising the steps of:

generating an e-mail message;

comparing said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

identifying whether~~said e-mail message as potentially containing malware if at least one of~~:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously

generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said email message is identified as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

holding said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

10. (Original) A method as claimed in claim 9, wherein said e-mail message specifies a plurality of addressees, said plurality of addressees being compared with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

11. (Original) A method as claimed in claim 9, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

12. (Original) A method as claimed in claim 11, wherein said proportion of addressees within said address book is user specified.

13. (Cancelled)

14. (Previously Presented) A method as claimed in claim 9, wherein said quarantine period is user specified.

15. (Original) A method as claimed in claim 9, wherein when said e-mail message is identified as potentially containing malware, then a user message is generated seeking a confirmation input from a user of said client computer before said e-mail message is sent.

16. (Original) A method as claimed in claim 9, wherein when said e-mail message is identified as potentially containing malware, then an administrator warning message is sent to an administrator of said client computer regarding said e-mail message.

17. (Currently Amended) Apparatus for detecting e-mail propagated malware within a client computer, said apparatus comprising:

an e-mail generator operable to generate an e-mail message;

a comparitor operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

a malware identifier operable to identify whether~~said e-mail message as potentially containing malware if at least one of~~:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said malware identifier is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

a quarantine queue operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

18. (Original) Apparatus as claimed in claim 17, wherein said e-mail message specifies a plurality of addressees, said comparitor being operable to compare said plurality of addressees with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

19. (Previously Presented) Apparatus as claimed in claim 17, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

20. (Original) Apparatus as claimed in claim 19, wherein said proportion of addressees within said address book is user specified.

21. (Cancelled)

22. (Previously Presented) Apparatus as claimed in claim 17, wherein said quarantine period is user specified.

23. (Original) Apparatus as claimed in claim 17, comprising a confirmation input unit operable when said e-mail message is identified as potentially containing malware to generate a user message seeking a confirmation input from a user of said client computer before said e-mail message is sent.

24. (Original) Apparatus as claimed in claim 17, comprising an administrator warning unit operable when said e-mail message is identified as potentially containing malware to send an administrator warning message to an administrator of said client computer regarding said e-mail message.

25. (New) A computer program product as claimed in claim 1, wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing.

26. (New) A computer program product as claimed in claim 1, wherein said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment.

27. (New) A computer program product as claimed in claim 1, wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware.

28. (New) A computer program product as claimed in claim 27, wherein said message to said malware computer program provider includes a copy of said e-mail message.